PhD Open Days

Security and Privacy in the Internet of Things

PhD Program in Information Systems and Computer Engineering

Rui Claro (rui.claro@tecnico.ulisboa.pt)

Motivation

Recent advances in computing technologies have resulted in small, networked devices that can be embedded in everyday objects at a low cost. This **Internet of Things (IoT)** creates opportunities to monitor and control the environment, with many potential benefits in the management of energy and other resources. However, it also poses **novel security challenges** that need to be tackled, because the implications of attacks go beyond traditional data leaks.

Intrusion Detection System

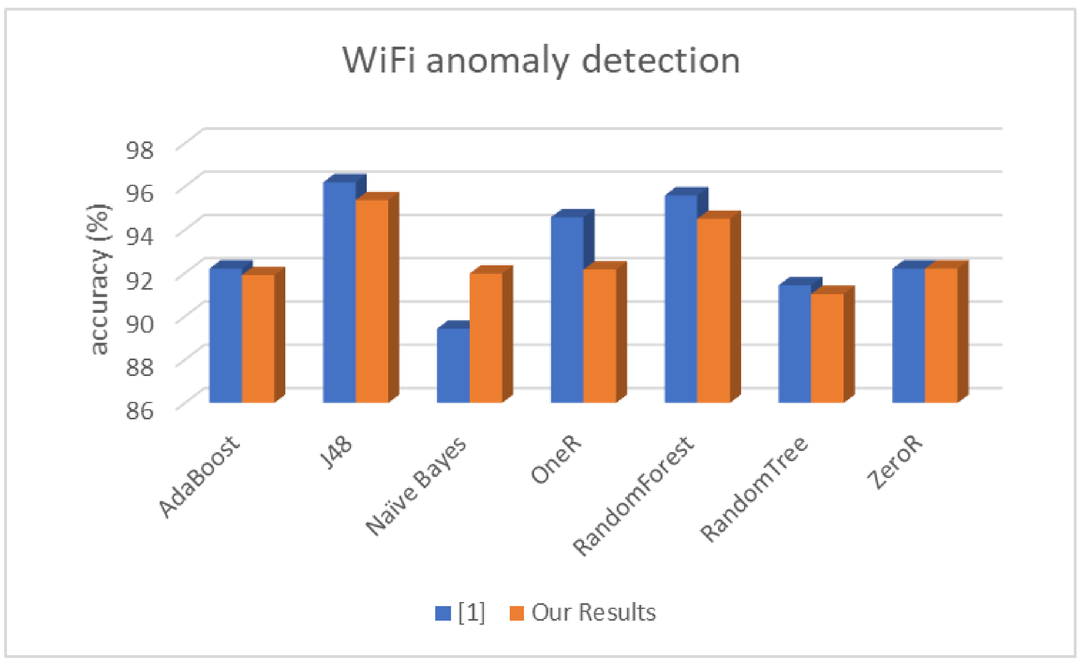
- Security concerns for communication using Wi-Fi
- IDS (Intrusion Detection Systems) are widely used for traditional network deployments, but not for small devices
- Are these solutions adaptable for the IoT environment?

AWID Dataset [1]

- Wi-Fi traces generated by traditional devices
- Including traces of 15 different Wi-Fi attacks

Anomaly-based detection

- Using most common machine learning algorithms
  - Adaboost, J48, Naive Bayes,
  - OneR, ZeroR, Random Tree and Random Forest



Fingerprinting

- Device identification with different levels of granularity
  - From category to a specific instance

In the **IoT** setting:

- Fingerprinting used for indoor location, network mapping

- But **HOW UNIQUE** are these fingerprints?

Physical Unclonable Functions

- Physical variations occur during semiconductor manufacturing
- Digital fingerprint based on those variations
  - Considered **UNIQUE** and hard to replicate

In the **IoT** setting:

- Used to create cryptographic keys based on chip configuration
- Can we use **fingerprinting** to create **Virtual PUFs**?
  - Can we use them in cryptography?

Related Work

Fingerprinting	PUF applications
IoTSense [2] - Behavioral fingerprinting.	RF-PUF [5] - Authentication of wireless nodes
IoT SENTINEL [3] - Device type identification.	PUFSec [6] - Key generation.
DEFT [4] - Distributed fingerprinting.	Spacial reconf. PUF [7] - Authentication.

Future Work

- Expand IDS work with data generated by IoT devices
- Continue research in Virtual PUFs

References

[1] Kolias, Constantinos, et al. "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset." IEEE Communications Surveys & Tutorials 18.1 (2016): 184-208

[2] Bezawada, Bruhadeshwar, et al. "Iotsense: Behavioral fingerprinting of iot devices." arXiv preprint arXiv:1804.03852 (2018)

[3] Miettinen, Markus, et al. "IoT Sentinel: Automated device-type identification for security enforcement in IoT." 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2017

[4] Thangavelu, Vijayanand, et al. "DEFT: A Distributed IoT Fingerprinting Technique." IEEE Internet of Things Journal 6.1 (2019): 940-952

[5] Chatterjee, Baibhab, Debayan Das, and Shreyas Sen. "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning." 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2018

[6] Park, So-Yeon, et al. "PUFSec: Device fingerprint-based security architecture for Internet of Things." IEEE INFOCOM 2017-IEEE Conference on Computer Communications. IEEE, 2017

[7] Babaei, Armin, and Gregor Schiele. "Spatial Reconfigurable Physical Unclonable Functions for the Internet of Things." International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, Cham, 2017

This work is supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UID/CEC/50021/2019 & with project reference PTDC/CCI-COM/31440/2017.

Supervisor: Miguel L. Pardal

PhD Program in Information Systems and Computer Engineering

phdopendays.tecnico.ulisboa.pt